Research Note

Understanding the SEC's Inadequate Internal Controls

Miranda Lin

Written: October 2017
Published: February 2018

Keywords: Internal Controls; Risk Management; Organizational Risk; Due Care; Risk Culture

Abstract: This paper discusses recent risk-related incidents at the U.S. Securities and Exchange Commission (SEC), and the apparent lack of adequate internal controls enforced within the organization. The author identifies some of the possible improvements to be made to the SEC's internal controls environment regarding their people, process, and systems.

Introduction

The U.S. Securities and Exchange Commission (SEC)'s mission is to "protect investors, maintain fair, orderly, and efficient markets, and facilitate capital information" by helping investors and the public understand publicly traded companies' past and current state, as well as directions for future development.[1] One of the most important platform the SEC uses to electronically collect data from companies is the Electronic Data Gathering Analysis and Retrieval (EDGAR) system, where companies send in information such as their income statements, and EDGAR performs "automated collection, validation, indexing, acceptance, and forwarding of submissions."[2] Containing such valuable data, EDGAR is a target for hackers by nature. On September 20 2017, the SEC disclosed through a public statement by its chairman Jay Clayton that a breach on EDGAR occurred sometime in 2016. Though detected in 2016, Clayton claimed that they did not conclude until August of 2017 that the "software vulnerability in [their] test filing component of [their] EDGAR system...was exploited and resulted in access to nonpublic information," which "may have provided the basis for illicit gain through trading."[3] The SEC provided very limited information regarding the breach, leaving out details such as the exact month and date of breach and possible suspects, but there is something we do know: there are numerous improvements to be made to the SEC's internal controls environment regarding their people, process, and systems.

SEC Internal Controls Environment

This is not the first time the SEC has experienced problems with protecting sensitive data, and the likelihood future security complications based on their current state seems high. Vulnerabilities exist due to negligent behavior of select employees as well as seemingly weak risk management culture. For example, in 2014 it was discovered that some of the Commission's employees lost their laptops, which "may have contained nonpublic information." Additionally, there were situations where SEC employees "sent nonpublic information through non-secure personal email accounts."[4] Based on these incidents, it is reasonable to conclude that within the SEC there is insufficient attention paid to the principle of due care: "the conduct that a reasonable person will exercise in a particular situation in looking out for the protection of things or the safety of others."[5] To encourage employees to practice due care and to strengthen their risk management culture, the SEC needs to re-evaluate the "degree to which it is instilling risk management behaviors into its culture...and how thoroughly it is practiced at all levels of the

organization."[6] If the SEC's leaders can "embrace and demonstrate appropriate enterprise risk management behaviors," the trickle-down effect will allow its employees to follow the tone, thus encouraging employees to act in accordance to best practices.[7]

On the other hand, the SEC's process and procedural controls are also inadequate. For instance, though the SEC developed information security policies, they do not appear to fully adhere to these policies. The U.S. Government Accountability Office (GAO)'s assessment conducted on the SEC in 2016 revealed that the SEC's disaster recovery plans were not "fully reviewed, completed, or up-to-date."[8] Additionally, in the report published on July 27 2017, the GAO stated that the SEC did not update their "network diagrams and asset inventories...to...reflect [their] current operating environment."[9] This raise questions as to whether the SEC can fully account for the risks inherent to their organization if they do not have a complete picture of their technology environment to aid in the process. Evidently, the Commission does not have enough oversight over their policies to ensure that their information security plans are updated. To achieve this and to develop defined processes for the organization to follow, the SEC should utilize the RACI model (responsibility assignment matrix) to identify who is responsible for updating security plans, who is accountable for oversight and approval of plans, who to consult with over concerns, and lastly, who communicates out these plans and to whom. At the minimum, these security plans should be reviewed and updated annually. Plans and policies are only useful if they are current and complete; the process of completing and updating security plans can only be accomplished with sufficient controls in place.

Regarding the SEC's technological systems, opportunities exist as well for improvement. The risks associated with a weak technical infrastructure "is relative based on the domain in which it is operated and the jurisdiction in which it thrives."[10] In the SEC's domain, privacy is at the greatest risk, yet the GAO reported in both 2016 and 2017 that the SEC failed to "encrypt sensitive information while in transmission" as well as had "confidential information stored on servers."[11] Considering that data encryption is one of the most standard best practices for protecting data, the SEC's insufficiency in this area cannot be tolerated. Besides encryption, the agency also has issues with authentication and authorization, for it did not "consistently identify and authenticate users" and "authorize access to resources."[12] To address the issue of authentication, the Commission needs to ensure that multi-factor authentication is in place. Adding an extra layer of identity verification will certainly reduce the likelihood of unauthorized access to the most confidential databases. As for the issue of authorization, the SEC needs to act in accordance with the principle of least privilege to guarantee that "only the minimum necessary rights [will] be assigned to a subject" for "access to a resource."[13] Not only does applying the principle of least privilege prevent unauthorized personnel from accessing sensitive data they do not need, it also ensures that authorized personnel only have access to the data for as long as their work requires.

Further problems involving the agency's data infrastructure exist. The GAO discovered that "13 of 42 user accounts reviewed had the same default password in the three key financial systems' servers" and that the SEC "did not disable these 13 active user accounts although they had never been used." In addition, the SEC did not consistently "protect its network boundaries from possible intrusions."[14] With fragile network boundaries, weak authentication for user accounts, combined with unencrypted data, the SEC's environment is welcoming to both internal and external hackers alike. Essentially, the door is wide open to everyone. Another issue common across the public sector is the use of outdated software, and the SEC is not excluded. They use some software programs that are no longer supported by the vendor, meaning that the vendor has also stopped releasing regular patches to bugs in the system.[15] With financial systems being such a significant part of its operations, it is surprising that the SEC has not yet addressed the risks of unpatched software and in fact continues to use it. The numerous inadequacies in their infrastructure as described can be attributed in part to the lack of directive and automated control activities; thus, it is essential that the Commission creates procedures for upgrading outdated software and securing network boundaries, such as adding additional layers of firewalls if possible. An IT configuration standard for strong

passwords and strong encryption of data is also necessary. Ultimately, these controls should be automated, where data encryption occurs automatically across all servers. Regarding passwords, users should be forced by the system to change the default password immediately after their account is issued, and should be forced to change their passwords periodically as well. Likewise, automatic system alerts should be configured to inform managers of user accounts that contain no activity for a reasonable period, so they can be checked, altered, or removed if no longer in use.

Recommendations

Externally, the SEC has voiced to provide "cybersecurity guidance to help...market participants protect their customers from cyber threats", but internally, the agency themselves could use some cybersecurity guidance.[16] There are reasonable information security improvements to be made. First, to keep the U.S.'s publicly traded companies' data secure in their database; the SEC needs to follow through with the enforcement of their own security policies. This means ensuring security policies & procedures, disaster recovery plans, network diagrams, and asset inventories are all complete and up to date. To do so, the agency needs stronger oversight over their projects. In particular, the SEC should use the RACI model to define and clarify all parties involved in each program, project, and plan. A re-examination of the technological systems also needs to be completed with stronger authentication, authorization, and encryption in mind. Specific directive and automated controls the SEC should review in their infrastructure include setting procedures for outdated software, establishing guidelines for stronger network boundaries, requiring strong, complex passwords on user accounts, leveraging the principle of least privilege for these accounts, implementing multi-factor authentication for confidential databases, and encrypting all information in servers. Lastly, the risk management culture throughout the SEC needs to be strengthened. The necessary culture change must come from the top; leading by example facilitates the improvement of employee behavior and adherence to internal controls. Employees often emulate the actions of leaders, and by doing so, the SEC could reduce and prevent situations such as negligently sending sensitive information over unsecured personal emails. With a strengthened risk management culture, behaviors that illustrate due care can and will be instilled into the agency. The SEC's important role as a watchdog over U.S. corporations is legitimate, but to support this role and set an example, they need to improve their own internal controls first. The agency receives and stores a significant amount of corporate information every year, and it is expected of them to implement strong controls to secure this confidential data and prevent unauthorized access and illicit use. By thoroughly re-examining their current situation and both identifying and managing risks, the SEC can reduce the likelihood of incidents like the 2016 EDGAR breach.

---

[1] "What We Do." U.S. Securities and Exchange Commission. 10 Jun. 2013. Accessed 14 Oct. 2017 <www.sec.gov>.

[2] "Everything EDGAR." U.S. Securities and Exchange Commission. 6 Jan. 2017. Accessed 14 Oct. 2017 <www.sec.gov>.

[3] "Statement on Cybersecurity." U.S. Securities and Exchange Commission. 20 Sept. 2017. Accessed 14 Oct. 2017 <www.sec.gov>.

[4] Isidore, Chris. "Why the SEC Hack is a Really Big Deal." *CNNMoney*. 21 Sept. 2017. Accessed 20 Oct. 2017 <money.cnn.com>.

[5] Albin-Wurzer, Melissa, et al. "2014 Information Security and Privacy Report." UW Office of the Chief Information Security Officer. 2014. Accessed 7 Oct. 2017 <ciso.uw.edu>.

[6] Coffin, Bill, et al. "The 2008 Financial Crisis: A Wakeup Call for Enterprise Risk Management." The Risk and Insurance Management Society. 2009. Accessed 30 Sept. 2017 <www.rims.org>.

[7] *Ibid.*

[8] "Opportunities Exist for SEC to Improve its Controls Over Financial Systems and Data". U.S. Government Accountability Office. 28 Apr 2016. Accessed 17 Oct. 2017 <www.gao.gov>.

[9] "SEC Improved Control of Financial Systems but Needs to Take Additional Actions." U.S. Government Accountability Office. 27 Jul 2017. Accessed 17 Oct. 2017 <www.gao.gov>.

[10] Atluri, Indrajit. "Managing the Risk of IoT: Regulations, Frameworks, Security, Risk and Analytics". ISACA Journal, Volume 3. 2017. Accessed 15 Oct. 2017.

[11] "SEC Improved Control of Financial Systems but Needs to Take Additional Actions."

[12] Ibid.

[13] Barnum, Sean, and Gegick, Michael. "Least Privilege". US-CERT. 10 May 2013. Accessed 23 Oct. 2017 < https://www.us-cert.gov/bsi/articles/knowledge/principles/least-privilege>.

[14] "SEC Improved Control of Financial Systems but Needs to Take Additional Actions."

[15] *Ibid*.

[16] "Cybersecurity, the SEC and You". U.S. Securities and Exchange Commission. 02 Oct. 2017. Accessed 22 Oct. 2014 < https://www.sec.gov/spotlight/cybersecurity>.